AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A method for generating ~~electronic~~ cryptographic keys from two integers a, b that are co-prime with one another, ~~the method comprising a step of verifying the co-primeness of said numbers a, b,~~ which includes the following operations:

A) - calculating the modular exponentiation $a^{\lambda(b)}$modb, where λ is the Carmichael function,

B) - verifying ~~that~~ whether this modular exponentiation is equal to 1,

C) - ~~retaining the pair a, b when equality is verified, and~~

[[D) –]] reiterating operations A and B with another pair of ~~numbers~~ integers when the modular ~~expansion~~ exponentiation is not equal to 1[[.]]; and

D) – generating at least two cryptographic keys from the integers a and b when the equality is verified.

2. (Original) A method for generating electronic keys according to Claim 1, wherein:

- an integer number b with a given length is chosen and is stored in memory,

- an integer number a is drawn at random,

- $a^{\lambda(b)}$modb is calculated,

- it is verified that $a^{\lambda(b)} = 1$ modb (or $a^{\lambda(b)}$modb = 1),

- the number a is stored in memory in the case where equality is verified,

- the above steps are reiterated with another number a when equality is not verified.

3. (Currently Amended) A method for generating electronic keys according to Claim 1, wherein the ~~number~~ integer b is predetermined, and the value λ(b) is calculated in advance and stored in memory.

4. (Currently Amended) The method of claim 1 further including the steps of encrypting and/or decrypting information by means of a public key cryptography protocol, using said ~~integers~~ cryptographic keys as the encryption and decryption keys.

5. (Currently Amended) A method for generating RSA or El Gamal or Schnorr cryptographic keys, comprising the steps of:

A) - selecting two integers a, b as candidates ~~for the keys~~;

B) - calculating the modular exponentiation $a^{\lambda(b)}$modb, where λ is the Carmichael function,

C) - verifying ~~that~~ whether this modular exponentiation is equal to 1,

D) - retaining the pair a, b when equality is verified, ~~and~~

E) - reiterating steps B and C with another pair of numbers when the modular expansion is not equal to 1[[.]], and

F) - generating at least pair of cryptographic keys from the pair a, b retained in step D.

6. (Original) A portable electronic device comprising an arithmetic processor and an associated program memory that are capable of effecting modular exponentiations, and further including a program for verifying the co-primeness of integer numbers of given length, which performs the following operations:

A) - calculating the modular exponentiation $a^{\lambda(b)} \bmod b$, where λ is the Carmichael function,

B) - verifying that this modular exponentiation is equal to 1,

C) – storing the pair a, b in the arithmetic processor when equality is verified, and

D) – reiterating steps A and B with another pair of integers when equality is not verified.

7. (Original) A portable electronic device according to Claim 6, wherein the number b is predetermined and the value λ(b) is calculated in advance and stored in a memory.

8. (Original) A portable electronic device according to Claim 6, wherein said portable electronic device comprises a chip card with a microprocessor.

9. (New) The portable electronic device of claim 6 wherein said arithmetic processor generates a pair of cryptographic keys from the stored pair of integers a, b.